*****PUBLIC VERSION*****

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA,

Plaintiff,

v.

ZACKARY ELLIS SANDERS,

Defendant.

Case No. 1:20-cr-00143
The Honorable Judge Ellis
Hearing: Sept. 11, 2020

MR. ZACKARY ELLIS SANDERS'S MOTION TO SUPPRESS BASED ON MATERIALLY MISLEADING STATEMENTS AND OMISSIONS REGARDING TOR, THE TARGET WEBSITE, AND THE SUBJECT PREMISES (Motion to Suppress No. 3)

Jonathan Jeffress (#42884)
Emily Voshell (#92997)
Jade Chong-Smith (admitted *pro hac vice*)
KaiserDillon PLLC
1099 14th Street. NW
8th Floor West
Washington, D.C. 20005
Telephone: (202) 683-6150
Facsimile: (202) 280-1034

Counsel for Defendant Zackary Ellis Sanders

TABLE OF CONTENTS

EXHIBITS INDEX

Exhibit #	Title
1	[redacted]
2	[redacted]
3	[redacted]
4	Declaration of Dr. Matthew Miller
5	Second Declaration of Dr. Matthew Miller
6	Fourth Declaration of Dr. Matthew Miller
7	Declaration of Seth Schoen
8	Declaration of Dr. Richard Clayton
9	[redacted]
10	[redacted]

Zackary Ellis Sanders, by and through undersigned counsel, and pursuant to Federal Rule of Criminal Procedure 41 and the Fourth Amendment, respectfully moves this Court to suppress all evidence and illegal fruits obtained pursuant to the invalid search warrant issued in this case because it was based on materially misleading statements and omissions regarding Tor, the Target Website [redacted] and the Subject Premises (the Sanders's family home). These material misleading statements and omissions were essential to the Magistrate finding probable cause to issue the search warrant in this case.

INTRODUCTION

The Federal Bureau of Investigation ("FBI") was investigating a [redacted]

[redacted]

Based on the scant discovery the Government has provided to date, the Government's own statements, and the declarations submitted by three defense experts,[1] Mr. Sanders has made "a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit." *Franks v. Delaware*, 438 U.S. 154, 155–56 (1978). The Affidavit misled the Magistrate into drawing inferences the Special Agent knew were incorrect that were essential to probable cause. Particularly when the false statements are excised from the Affidavit and the material omissions are added, there was no basis for probable cause and no neutral Magistrate would have issued the warrant. As a result, Mr. Sanders requests, and is respectfully entitled to, a *Franks* hearing. *Id.* ("if the allegedly false statement is necessary to the finding of probable cause, the Fourth Amendment requires that a hearing be held at the defendant's request").

Because the warrant was based on materially false statements and omissions, the good faith exception under *United States v. Leon*, 468 U.S. 897, 932 (1984) does not apply. As a result, all evidence derived from the illegal search of the Sanders's family home, the interrogation of Mr. Sanders and his parents, and the forensic examinations of any tangible evidence should be suppressed as fruit of the poisonous tree.

[1] The declarants are Dr. Matthew Miller, Associate Professor Computer Science and Information Technology at the University of Nebraska at Kearney; Seth Schoen, computer technologist and privacy specialist who worked as a Senior Staff Technologist at the Electronic Frontier Foundation for the past 19 years; and Dr. Richard Clayton, Director of the Cambridge Cybercrime Centre at the University of Cambridge.

BACKGROUND[2]

A. THE TOR NETWORK

"Tor" originally stood for "The Onion Routing,"[3] because the network provides security by encasing data that travels through the network in different layers of encryption, like an onion: these layers of encryption are gradually unpeeled at different points in the random circuit of at least three of the thousands of volunteer-run nodes around the world that comprise the Tor network. *See* Ex. 8 (Declaration of Dr. Richard Clayton) at 3-4 (explaining how data that travels on the Tor network is encrypted in what is best analogized as a "three-layer 'onion'"). As this Court has previously acknowledged, "[t]he U.S. Naval Research Laboratory created the Tor network in an attempt to protect government communications. The public now can access the Tor network. Many people and organizations use the Tor network for legal and legitimate purposes." *United States v. Matish*, 193 F. Supp. 3d 585, 593 (E.D. Va. 2016).

The Tor network "provides anonymity to users of the network" through at least three random nodes that comprise what is called a Tor circuit. Ex. 6 (Fourth Declaration of Dr. Matthew Miller) at 2-3. Thus, "[w]hen someone visits a web site using the Tor Browser, all the communications with the web site are sent through . . . three or more randomly chosen Tor nodes, out of the thousands that make up the Tor network, passing through them before arriving at their destination." Ex. 7 (Declaration of Seth Schoen) at 1-2.

The way the Tor network works when an Internet user browses the Internet on the Tor network is best explained by an analogy to mail: "[t]he routing of the packets [of data] from the Internet user, through the Tor circuit, to a website is like opening an envelope, which contains 2

[2] Mr. Sanders also hereby incorporates by reference the background section of the Memorandum in Support of his Motion to Suppress Due to Lack of Probable Cause (Motion to Suppress No. 1).

[3] *History*, the Tor Project, https://www.torproject.org/about/history/ (last accessed Aug. 18, 2020).

other progressively smaller envelopes, the last of which contains the request to be sent to the website." Ex. 6 (Fourth Declaration of Dr. Matthew Miller) at 2. However, in this analogy, "[e]ach envelope does not reveal the recipient or the contents of the next smaller envelope." *Id.* at 2. Thus, as Dr. Miller explains in further detail:

> When an Internet user visits a website through the Tor Network, the Internet user's request is sent to that website by traveling from the Internet user to node 1, from node 1 to node 2, from node 2 to node 3, and then from node 3 to the website. When the Tor Browser sends packets of data through the Tor Network, it has to encrypt the packets of data in the reverse order they travel in. The Internet user's request (packets of data) to the website is placed on an un-encrypted postcard (Postcard #1), where the return address is node 3 and the recipient address is to the website. Postcard #1 is encased in an encrypted envelope (Envelope #3), where the return address is node 2 and the recipient address is node 3. Envelope #3 is encased in an encrypted Envelope #2, where the return address is node 1 and the recipient address is node 2. Envelope #2 is encased in an encrypted Envelope #1, where the return address is the Internet user and the recipient address is node 1.

Id. at 2.

Dr. Richard Clayton provides "a real-world example of what one node within a TOR network does" to further illustrate this process:

> an anonymous Valentine can be sent by putting the card into an envelope and addressing it to its destination. This can then be put into another envelope and sent to a small town in Texas. The outer envelope will be opened and the post office will frank the inner envelope "Valentine, TX" and the card will then be delivered by the Post Office to its destination. Inspecting the outer envelope does not reveal the inner envelope's destination – and the card's recipient does not know in which town the sender resides. Further, since envelopes come in a small range of standard sizes, someone watching all the mail would not be able to track any particular envelope merely by measuring it.

Ex. 8 (Declaration of Dr. Richard Clayton) at 4.

While "the Tor network's privacy features make it more difficult to count its users compared to other software and services, available statistics suggest that the Tor network is currently used by about 2.5 million people each day." Ex. 7 (Declaration of Seth Schoen) at 2; *see also* Ex. 8 (Declaration of Dr. Richard Clayton) at 7 (similar).

B. THE TOR PROJECT

The Tor Project is a 501(c)(3) non-profit organization that supports the Tor network and the Tor Browser to protect freedom online. The Tor Project's mission is "[t]o advance human rights and freedoms by creating and deploying free and open source anonymity and privacy technologies, supporting their unrestricted availability and use, and furthering their scientific and popular understanding."[4] As part of the mission, the Tor Project was "the main developer of the Tor Browser and the software behind the Tor Network." Ex. 7 (Declaration of Seth Schoen) at 1. The Tor Project developed the Tor Browser to provide the public with easy access to the Tor Network and heightened anonymity protections when browsing online. *Id.* Today, the Tor Project promotes, supports and provides downloads for the Tor Browser. *Id.*

1. The U.S. Government Is And Has Been One Of The Main Sponsors Of The Tor Project.

The U.S. government has been one of the main proponents and supporters of Tor. The first onion routing network design and prototype was created by the U.S. Naval Research Laboratory in the mid-1990s.[5] It was designed to provide Internet users with maximum privacy by routing Internet traffic through multiple servers. Since then, other researchers, developers, and organizations have sought to build on that work, most notably the Tor Project. In 2006, the Tor Project obtained its 501(c)(3) status and The Tor Project was established as a non-profit to support

[4] *Browse Privately. Explore Freely*, The Tor Project, https://www.torproject.org/ (last accessed Aug. 13, 2020); Ex. 7 (Declaration of Seth Schoen) at 2; Ex. 6 (Fourth Declaration of Dr. Matthew Miller) at 3.

[5] *History*, the Tor Project, https://www.torproject.org/about/history/ (last accessed Aug. 18, 2020).

the development of the Tor network and the Tor Browser. The Tor Project has been heavily funded by the U.S. government "to promote Internet freedom." Ex. 7 (Declaration of Seth Schoen) at 2.

Some of the active sponsors who fund The Tor Project's work today include the U.S. government, educational institutions, philanthropies, and well-known publicly traded companies. For example, current active sponsors include the U.S. Department of State Bureau of Democracy, Human Rights, and Labor; the Media Democracy Fund; the Defense Advanced Research Projects Agency via Georgetown University; the National Science Foundation via Georgetown University; the Institute of Museum and Library Services via New York University; Craig Newmark Philanthropies; and the Google Summer of Code program.[6]

2. Neither The Tor Network Nor The Tor Browser Are Designed Or Primarily Used For Illegal Purposes.

Neither the Tor network nor the Tor Browser are designed or primarily used for illegal activities. Rather, "Tor has been developed to be a tool for free expression, privacy, and human rights. It is not a tool designed or intended to be used to break the law, either by Tor users or Tor relay operators."[7] Indeed, the vast majority of people (over 96%) who use the Tor network and Tor Browser do so to visit websites on the open Internet with the heightened anonymity protections that Tor provides. "[H]idden service traffic is about 3.4 percent of total Tor traffic, which means that, at least according to our early calculations, 96.6 percent of Tor traffic is []not[] hidden services . . . In other words, the majority of Tor traffic comes from users that are using the network to browse the public-facing web anonymously, and not by those accessing hidden sites").[8] Of the

[6] *Sponsors*, The Tor Project, https://www.torproject.org/about/sponsors/ (last accessed Aug. 13, 2020); *see also* Ex. 7 (Declaration of Seth Schoen) at 2 (similar).

[7] *The Legal FAQ for Tor Relay Operators*, the Tor Project, https://community.torproject.org/relay/community-resources/eff-tor-legal-faq/

[8] Matthew Braga, *Most Tor Traffic isn't going to the Dark Web, Data Suggests*, Vice (Feb. 27, 2015), https://www.vice.com/en_us/article/9ak8av/most-tor-traffic-isnt-going-to-the-dark-web-data-suggests (quotation marks omitted).

less than four percent of Tor Onion Service websites that make up traffic on the Tor network, the majority of such websites (52%) are legal under both U.S. and U.K. law.[9]

C. THE TOR BROWSER

The Tor Browser is a software application that people use to access the Tor network and thereby browse websites on both the open Internet (what people usually think of when they think of the Internet) and Tor Onion service websites. *See, e.g.*, Ex. 4 (Declaration of Dr. Matthew Miller) at 2 ("The Tor Browser is a browser that uses the Tor Network to connect to the Internet. It has the ability to browse 'open' Internet websites as well as Tor Onion Service websites"). [redacted]), Internet users could visit it, other Tor Onion Service websites, or open Internet websites by connecting to the Tor network through the Tor Browser.

1. There Are Many Legitimate Reasons For People To Use The Tor Browser To Connect To The Tor Network.

Protecting the anonymity of a user's IP address is a design feature of both the Tor network and the Tor Browser, and it is what provides people with many legitimate reasons for downloading and using the Tor Browser to access the Tor network. Ex. 7 (Declaration of Seth Schoen) at 4. Because people's activities online can otherwise be tracked, people who want to control what information they share about themselves can use the Tor Browser to make sure their information isn't exposed or tracked in ways they don't want." *Id.* at 2. For example, people may use Tor to protect their anonymity because:

> Many people don't want the things they say online to be connected with their offline identities. They may be concerned about political or economic retribution, harassment, or even threats to their lives. Whistleblowers report news that companies and governments would prefer to suppress; human rights workers

[9] Larry Loeb, *Study Shows Dark Web Isn't as Large or Illegal as Previously Thought*, Security Intelligence (Apr. 12, 2016), https://securityintelligence.com/news/study-shows-dark-web-isnt-as-large-or-illegal-as-previously-thought/.

> struggle against repressive governments; parents try to create a safe way for children to explore; victims of domestic violence attempt to rebuild their lives where abusers cannot follow.[10]

Anonymizing online activities can enable people to more freely communicate, organize, and associate with others. Using a Tor browser can create space for people to develop and share ideas. In particular, people who are members of minority groups who may fear discrimination or harassment on the basis of their sexual orientation, ethnicity, race, religion, or gender identity can feel more empowered to exercise their First Amendment rights in such spaces. *See, e.g.*, *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 357 (1995) (explaining, in a different context, how "[a]nonymity is a shield from the tyranny of the majority. . . . It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation—and their ideas from suppression—at the hand of an intolerant society").

As another example of why people would legitimately use the Tor Browser, it helps people keep private information that companies would otherwise seek to collect to profile people and target advertisements towards them. If people want to search for sensitive information, such as information about "erectile dysfunction, herpes, adult incontinence, bankruptcy, gay bars, BDSM, fertility issues, pregnancy, or abortion," if they use the Tor Browser to search for such information it will help "break the connection between the sensitive topic and the identity of the person doing the search" and thereby avoid "repeatedly being shown uncomfortably revealing ads on the topic in the future." Ex. 7 (Declaration of Seth Schoen). at 2. In addition to using the Tor Browser to keep private personal information and avoid targeted ads, people also use it to keep their location

[10] *Anonymity*, Electronic Frontier Foundation, https://www.eff.org/issues/anonymity (last accessed Aug. 19, 2020).

private, see what websites look like from elsewhere in the world, avoid Internet censorship, do research without revealing where they work, and provide anonymous tips to media or law enforcement. *Id.* at 3-4. People use Tor for these reasons precisely because Tor allows people to keep their identity and activities private by protecting the anonymity of the IP addresses of the devices they use. *Id.* at 4.

2. The Tor Browser Is A Non-Default Browser (Like Google Chrome Or Mozilla Firefox) But, Compared To Other Browsers, It Has Heightened Privacy And Security Protections.

The Tor Browser is a non-default browser that allows people to easily access the Internet and make choices about what they reveal about themselves—and what they do not—to advertisers, private corporations, data brokers, websites, and anyone else who is otherwise monitoring, drawing inferences from, and even profiting off of people's activities online. *Id.* at 2-4; *see also* Ex. 6 (Fourth Declaration of Dr. Matthew Miller) at 3. It is similar in some ways to other web browsers, like Internet Explorer, Apple Safari, Mozilla Firefox, Google Chrome, and Microsoft Edge, in that it allows Internet users to access the Internet. Indeed, the Tor Browser is actually an enhanced version of Mozilla Firefox. Ex. 7 (Declaration of Seth Schoen) at 4; Ex. 8 (Declaration of Dr. Richard Clayton) at 5. Non-Tor browsers, such as the ones previously described, lack the heightened privacy and security settings of the Tor Browser. The Tor Browser allows Internet users to access (via the Tor network) both open Internet websites and Tor Onion Service websites.

Like Mozilla Firefox and Google Chrome (but unlike Internet Explorer, Apple Safari, or Microsoft Edge), the Tor Browser is a non-default web browser, which means that it does not automatically come installed on a device when someone purchases it. People who want to use a non-default browser need to take affirmative steps to download one.

The Tor Browser is considered a better browser than the default browsers that automatically come with devices (such as Internet Explorer, Apple Safari, or Microsoft Edge) and better than other non-default browsers (such as Mozilla Firefox and Google Chrome). For example, Fox News compared which was the best of different web browsers and gave the Tor browser an honorable mention: Fox News reported that the "Tor Browser is one of the best anonymous web browsers out there. It's so reliable, in fact, that people living under repressive governments have used it to break through censorship. . . if you're looking for the safest, most private way to browse the net, Tor might be your go-to."[11] Furthermore, Fox News noted that while Apple Safari and Microsoft Edge are the "default" browsers that usually "come bundled with new computers, . . . they tend to lack some of the security features and extensions" found in other browsers one can download.[12] Fox News further counselled against using a default browser such as Internet Explorer, giving it a dishonorable mention, in part because it is "an absolute minefield for malware."[13]

The Tor Browser has heightened privacy and security for a number of reasons. It allows an Internet user to browse the Internet via the Tor network. It "does not (1) save an Internet user's search history in the browser itself as the Internet user is browsing or (2) save search history or cache images to the hard disk of the Internet user's computer," in order to ensure "that an Internet user does not reveal their search history or what they have done on the Internet" and thereby

[11] *Which browser is best? Comparing Chrome, Safari, Firefox, Edge, and Tor*, Fox News, https://www.foxnews.com/tech/which-browser-is-best-comparing-chrome-safari-firefox-edge-and-tor (last accessed Aug. 13, 2020).

[12] *Id.*

[13] *Id.*

"protect [an] Internet user's anonymity." Ex. 6 (Fourth Declaration of Dr. Matthew Miller) at 3. It also "severely restrict[s]" the functionality of "code (especially JavaScript code) embedded into websites" in order to protect the anonymity of an Internet user's IP address. Ex. 8 (Declaration of Dr. Richard Clayton) at 5.

3. The Tor Browser Is Easy To Download.

It is simple for anyone to download the Tor Browser—even if they are not technically sophisticated—on their computer, mobile phone, or other web-accessible device. Ex. 7 (Declaration of Seth Schoen) at 4. For example, a person can go to the Tor Project website, at https://www.torproject.org/download/, and with one or two clicks[14] download the Tor Browser for free. Downloading the Tor Browser from the Tor Project website takes no more than a few minutes. Ex. 7 (Declaration of Seth Schoen) at 5-6 (describing the steps required to download the Tor Browser and providing screenshots to provide a visual explanation).

4. The Steps Required To Download The Tor Browser Are The Same Steps Required To Download Any Other Non-Default Browser.

Downloading a web browser is the same process whether someone is downloading the Tor Browser or another non-default browser like Mozilla Firefox or Google Chrome. *Id.* at 4 ("The steps to download and use the Tor Browser are the same as those to download and use any other Browser"); *see also id.* at 5-6 (depicting and explaining the steps required to download the Tor Browser).[15]

5. The Tor Browser Is Easy To Use.

[14] Some browsers (and depending on how people have configured their browsers) will ask a person to confirm that they want to download a file, while others will immediately start downloading after a person click the download button.

[15] If someone wanted to download Google Chrome or Mozilla Firefox, someone would simply need to search for "Google Chrome" or "Mozilla Firefox" in a search engine and then follow the same steps as described in Ex. 7 (Declaration of Seth Schoen), *i.e.* they would simply visit the relevant download page and download the software.

The Tor Browser was specifically designed to be as easy to use as any other non-default browser, so that the public could have free, easy-to-access, heightened security protections while browsing online. *Id.* at 4; *see also* Ex. 8 (Declaration of Dr. Richard Clayton) ("Using TOR is extremely easy – one downloads the 'TOR bundle for Windows, Mac or for one's phone or tablet. One then installs it and launches it and it can immediately be used. On a fast connection this takes less than a minute"). Once a person has downloaded the Tor Browser, to browse the Internet they simply need to open the program by clicking on its icon—just like they would for any other web browser. Ex. 7 (Declaration of Seth Schoen). at 7. "The Tor Project has continued to improve the ease of use and security of the Tor Browser since 2008. These enhancements to the Tor Browser are one of the Tor Project's core activities." *Id.* at 4.

One a person has opened the Tor Browser, it is similar to any other web browser. *See Id.* at 7 (providing a screenshot of the Tor Browser). There is a web address bar where a person can enter the address of the website they want to visit. *Id.* There is also a default search engine bar where a person can enter search terms. *Id.* For example, if a person used the default search engine bar, they could search for, for example, "eastern district of virginia u.s. district court" and the search engine would display the results. *See Id.* at 8 (providing a screenshot of search results on the Tor Browser). A person could then use the Tor Browser to visit this Court's website. *See Id.* at 9 (providing screenshot of the "Court's website as visited with the current version of Tor Browser" and noting "[t]he process of navigating to it, and the site's appearance, were much the same as in any other web browser"). There is also a search engine for Tor Onion Service websites, called Torch, which Internet users can find simply by searching "Tor search engine." A person could search for, for example, "department of justice" results on Tor Onion Service websites. *See Id.* at 12 (providing a screenshot of search results on the Tor Browser).

D. HOW PEOPLE BROWSE THE INTERNET.

When people "browse" the Internet, they do not always know what they are looking for: in fact, the very phrase "browsing the Internet" can "imply a sense of aimlessness, with the user just wasting time on the Internet."[16] Thus, "[b]ecause of how Internet users browse the Internet there are two main ways that they usually come across a website: 1) by using a search engine or 2) by clicking on a hyper-link (aka a link)." Ex. 6 (Fourth Declaration of Dr. Matthew Miller) at 6. People can and do click on links or even register for accounts without knowing where it will lead them. Ex. 5 (Second Declaration of Dr. Matthew Miller) at 2; *see also* Ex. 7 (Declaration of Seth Schoen) ("Internet users can easily visit web sites without knowing their contents, whether by clicking on search engine results or following a link that they found or received in some other way"). "Within Tor Browser, links to onion sites can be used and visited just like other web sites. For example, a Tor Browser user can navigate to one simply by clicking on a search engine result or other link." *Id.* at 11.

1. Search Engines.

People can use search engines to browse the open Internet and Tor Onion Service websites. *See, e.g.*, Ex. 7 (Declaration of Seth Schoen) at 11-12. Indeed, "there are search engines that do 'index' the contents of the Tor Network, including Tor Onion Services. Search engines create indexes which are like the yellow pages of the Internet. These indexes provide a brief description of the webpages, but search engines usually do not have access to password protected pages on a

[16] *Browsing*, Technopedia, https://techopedia.com/definition/797/browsing (last accessed Jul. 29, 2020).

website. Thus, they usually cannot view or describe the content that is password protected." Ex. 6 (Fourth Declaration of Dr. Matthew Miller) at 6-7.

When people use a search engine, such as Google, DuckDuckGo, or Torch, it is "not unusual for Internet users to receive search results that are different from what they expected, or to be confused about the nature of a particular search result, or to click on a search result that's not what they intended." Ex. 7 (Declaration of Seth Schoen) at 10. This is because "[m]any words and terms have multiple possible meanings, and these ambiguities create challenges for search engines and Internet users." *Id*. at 10. "For example, an Internet user might search for 'cardinals' or 'pictures of cardinals'. They might find or click on web sites dedicated to various kinds of cardinals: a common bird in North America, the St. Louis Cardinals baseball team, or the members of the College of Cardinals in the Roman Catholic Church." *Id.* at 10. Furthermore, search engine results for websites that require a login may not be accurate or make clear what the website will contain: "content that requires special access such as a login account is almost always invisible to web crawlers, and so not indexed by search engines and invisible to Internet users. For example, a search engine couldn't see the content of a private discussion forum that required a login." *Id.* at 10. (However, while the search engine's description of a website that requires a login to view will not be accurate because the password-protected content is invisible to the search engine, and therefore Internet users looking at search results, the website itself would still be indexed by the search engine).

2. Links.

"Users can, not uncommonly, get a [URL] link from a search engine or from another source and click on it without knowing any or all of the content that they'll find on that particular page." Ex. 7 (Declaration of Seth Schoen) at 11. People may not know where a URL link will lead because links are often “opaque,” meaning “there’s no way to tell what they lead to just by looking at them.” *Id.* at 11. A couple of examples help illustrate this point:

- “[B]oth of the video links https://www.youtube.com/watch?v=0Ak_7tTxZrk and https://www.youtube.com/watch?v=2mBF2gSEEHQ have a very similar appearance, with a meaningless data element at the end (“0Ak_7tTxZrk” and “2mBF2gSEEHQ”). One of these videos is a performance of a Beethoven piano sonata, while the other is footage of the August 2020 explosion in the port of Beirut.” *Id.* at 10-11.
- “[O]ne of https://bit.ly/2XRd3IU and https://bit.ly/3izBkv8 will send Internet users to this Court’s web site, while the other points them to a Rick Astley music video.” *Id.* at 11.
- [redacted] Ex. 7 (Declaration of Seth Schoen) at 10; *see also supra* at n.18.

In addition to URL addresses being ambiguous, hyperlinks can also be ambiguous. Hyperlinks “provide[] only a short description of where the user will go, but there could be different content hosted at the website. A common example would be the use of headlines in a newspaper article, where the headline would grab the reader’s attention, but only when they read the article, will they know the true story. A [hyper]link (like a headline) is a word or short phrase that cannot fully represent the content the user will view after clicking on the link.” Ex. 6 (Fourth Declaration of Dr. Matthew Miller) at 6. Thus, “[f]or example, a pornography website could be [hyper-]linked (described) as a BDSM website and just based on the text displayed to the Internet user, they would not know exactly what content they would find if they clicked on the [hyper-]link to that website." *Id.* at 6.

3. A One-Time Visit To A Website.

"Someone who visits a web site only once is more likely to have found the content of that site was either not what they expected or not what they were looking for, compared to someone who visits a web site repeatedly." Ex. 7 (Declaration of Seth Schoen) at 10.

THE LAW OF FRANKS V. DELAWARE

Mr. Sanders hereby incorporates by reference the section on the Law of *Franks v. Delaware* of the Memorandum in Support of his Motion to Suppress Based on Materially False and Misleading Information In [redacted] (Motion to Suppress No. 2).

ARGUMENT

I. THE AFFIDAVIT MISLED THE MAGISTRATE ABOUT TOR AND OTHER ISSUES MATERIAL TO PROBABLE CAUSE.

In addition to the false and misleading information in [redacted], which are addressed by separate motions,[17] the Affidavit misled the Magistrate about [redacted] Furthermore, the Special Agent also [redacted]. Without these misrepresentations and omissions, the Magistrate would not have found probable cause to issue the search warrant.

[17] *See* Motion to Suppress Based on False and Misleading Material Information in Affidavit [redacted] (Motion to Suppress No. 2) and Motion to Suppressed Based on False and Misleading Material Information in Affidavit Paragraph 25 (Motion to Suppress No. 4).

A. The Affidavit misled the Magistrate about Tor.

The Affidavit misled the Magistrate about Tor in [redacted], downloading and installing the Tor Browser requires the same steps (and is just as easy) as downloading and installing a non-default browser. Additionally, the steps required "to download the Tor Browser and access the Tor network are the same steps that a user would take in order to make use of Tor for any of the legitimate reasons" previously described. Ex. 7 (Declaration of Seth Schoen) at 5. [redacted] the origins of Tor, the mission and purpose of the Tor Project, the U.S. government's connection to the Tor network and Tor Project as a key sponsor and supporter, the many legitimate reasons that people download and use Tor, and the benefits that Tor provides in terms of anonymization that are not primarily intended to shield illegal activity.

The Affidavit's misleading statements and omissions [redacted] are material because the Affidavit was incorrectly asking the Magistrate to read suspicion into legitimate conduct that many people engage in every day. Had the Affidavit provided a more accurate and complete characterization of Tor, the Magistrate would have had a more complete understanding of why and how people use Tor and would have ultimately understood that [redacted]

1. The Affidavit misled the Magistrate about [redacted].

[redacted] *See, supra* at 27-29. [redacted]

[redacted]

[redacted].

2. The Affidavit misled the Magistrate about [redacted]

The Affidavit misled the Magistrate in [redacted]

[redacted]

[redacted]

[redacted]

3. The Affidavit misled the Magistrate about evidence [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

4. The Affidavit misled the Magistrate [redacted]

The Affidavit misled the Magistrate in [redacted]

[redacted]

[redacted]

[redacted]

5. The Affidavit misled the Magistrate by omitting information [redacted]

The Affidavit misled the Magistrate by failing to disclose [redacted]

[redacted]

[redacted]

6. The Affidavit misled the Magistrate through omissions that, taken together, were essential for the Magistrate to find probable cause.

As discussed elsewhere in this Motion, the Affidavit did not disclose to the Magistrate about information that, individually and especially when taken together, would have prevented the Magistrate from finding probable cause. For example, the Special Agent did not tell the Magistrate that: [redacted],

[redacted]

II. THE GOOD FAITH EXCEPTION DOES NOT APPLY.

The good faith exception to the exclusionary rule does not apply here. *See United States v. Leon*, 468 U.S. 897 (1984). Mr. Sanders hereby incorporates by reference the section on "The Good Faith Exception Does Not Apply" of the Memorandum in Support of his Motion to Suppress Based on False and Misleading Information In [redacted] Motion to Suppress No. 2).

III. ALL FRUITS OF THE ILLEGAL SEARCH MUST BE SUPPRESSED.

As a result of the invalid warrant, any evidence so derived must be suppressed as fruit of the poisonous tree.[18]

CONCLUSION

Because the warrant issued in this case was based on materially false statements and omissions, and because *even without correcting the Affidavit* it was "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable," *United States v. Leon*, 468 U.S. 897, 932 (1984), the good faith exception does not apply. As a result, all evidence derived from the illegal search of the Sanders's family home, the illegal interrogation of Mr. Sanders and his parents, and the illegal forensic examinations of any tangible evidence should be suppressed as fruit of the poisonous tree.

Respectfully submitted,

[18] Mr. Sanders hereby incorporates by reference the section "All Fruits of the Illegal Search Must be Suppressed" from the Memorandum in Support of his Motion to Suppress Due to Lack of Probable Cause (Motion to Suppress No. 1).

/s/ Jonathan Jeffress

Jonathan Jeffress (#42884)
Emily Voshell (#92997)
Jade Chong-Smith (admitted *pro hac vice*)
KaiserDillon PLLC
1099 Fourteenth St., N.W.; 8th Floor—West
Washington, D.C. 20005
Telephone: (202) 683-6150
Facsimile: (202) 280-1034
Email: jjeffress@kaiserdillon.com
Email: evoshell@kaiserdillon.com
Email: jchong-smith@kaiserdillon.com

Counsel for Defendant Zackary Ellis Sanders